Kassenärztliche Bundesvereinigung
Körperschaft des öffentlichen Rechts

Sicheres Netz der KVen

Richtlinie KV-SafeNet (Netzkopplung)

[KBV_SNK_RLEX_Netzkopplung]

Dezernat 6
Informationstechnik, Telematik und Telemedizin

10623 Berlin, Herbert-Lewin-Platz 2

Kassenärztliche Bundesvereinigung

Version	1.0
Datum:	31.10.2011
Klassifizierung:	Öffentlich
Status:	In Kraft

DOKUMENTENHISTORIE

Version	Datum	Autor	Änderung	Begründung	Seite
1.0	31.10.2011	KBV	Erstellung, Kommentierung, QS und Freigabe		alle

INHALTSVERZEICHNIS

A B B I L D U N G S V E R Z E I C H N I S

1 Präambel

1.1 Das *Sichere Netz der KVen*

Die Kassenärztliche Bundesvereinigung und die Kassenärztlichen Vereinigungen haben eine Online-Infrastruktur aufgebaut, die den hohen Anforderungen an Datenschutz und Datensicherheit Rechnung trägt und die u.a. für die Übermittlung von Patienten- und Honorardaten geeignet ist – das *Sichere Netz der KVen*.

Informationssicherheit im *Sicheren Netz der KVen* ist eines der wichtigsten Ziele aller Beteiligten. Von besonderer Bedeutung ist dabei der Schutz der Sozialdaten und weiterer personenbezogener Daten. Für diese und andere Informationen und Werte werden im Rahmen des Sicherheitsmanagements Schutzziele definiert. Im Mittelpunkt dabei stehen die Sicherung der Vertraulichkeit, die Gewährleistung der Integrität und die Aufrechterhaltung der Verfügbarkeit. Zur Einhaltung dieser Ziele trifft die KBV regulatorische Maßgaben in Form von Richtliniendokumenten und Zertifizierungen. Die Umsetzung obliegt allen Beteiligten.

Die Rechenzentren der Kassenärztlichen Vereinigungen (KVen) und der Kassenärztlichen Bundesvereinigung (KBV) sind hierzu über den KV-Backbone, einem logisch vom Internet getrennten Netzwerk, miteinander verbunden. Die KBV ist der Betreiber des KV-Backbones.

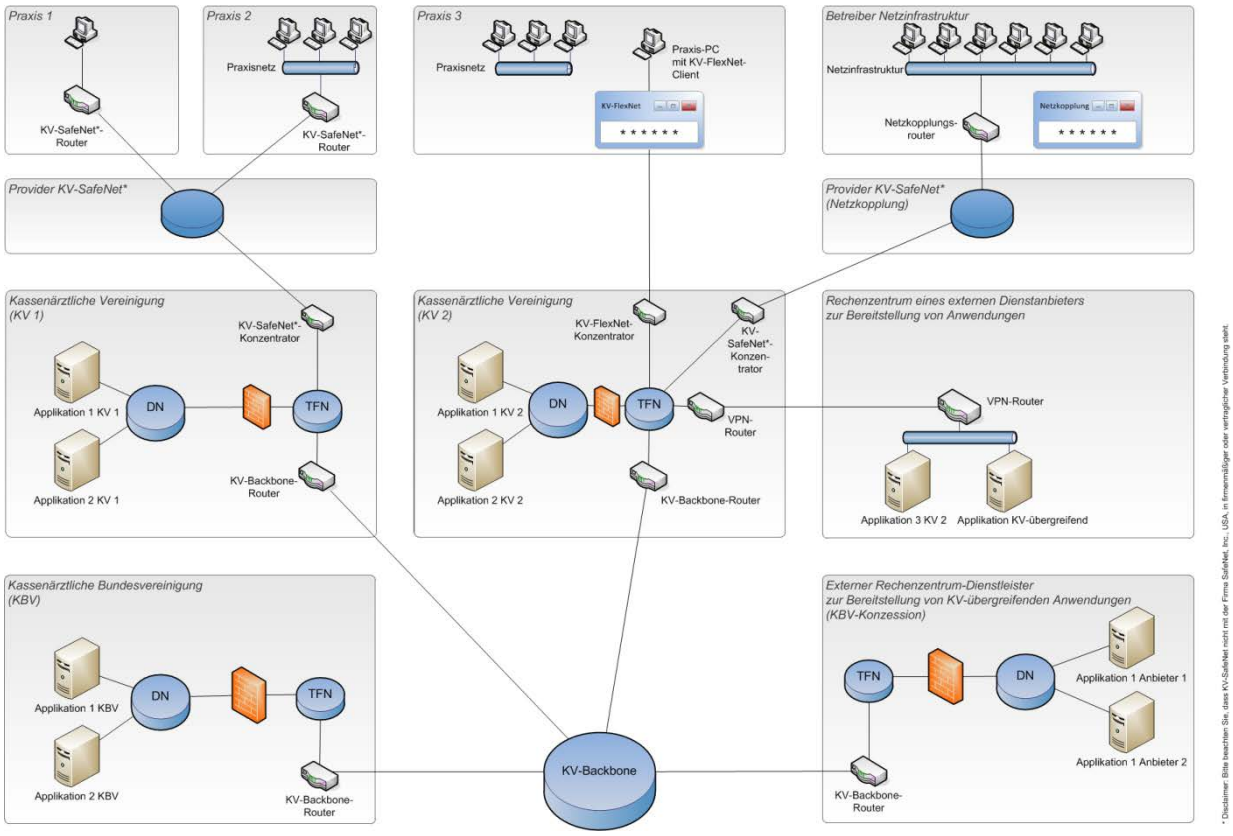

Abbildung 1: Beispielhafte Netztopologie

Teilnehmer am *Sicheren Netz der KVen* sind die Mitglieder der Kassenärztlichen Vereinigungen, also Vertragsärzte und –psychotherapeuten oder ein anderes nach den Richtlinien der KBV zugelassenes Mitglied des *Sicheren Netzes der KVen*. Ihnen werden sichere Zugangswege zu den Diensten und Anwendungen bereitgestellt. Die Anbindung der Teilnehmer an das *Sichere Netz der KVen* erfolgt mittels einer VPN-Verbindung. Es gibt hierbei zwei Mög-

lichkeiten der sicheren Anbindung, einerseits über das KV-SafeNet*, einem Hardware-VPN und andererseits über das KV-FlexNet[1] einem Software-VPN. Die Bereitstellung eines Zugangs über die Variante KV-FlexNet liegt in der Hoheit der jeweiligen KV. Beide Zugangsvarianten ermöglichen eine sichere Anbindung an das *Sichere Netz der KVen*.

Der Anschluss von Teilnehmern aus bereits in sich abgesicherten gesundheitsmedizinischen Netzinfrastrukturen an das *Sichere Netz der KVen* erfolgt mittels KV-SafeNet (Netzkopplung). Diese gesicherte Anbindung basiert auf der Zugangsvariante KV-SafeNet und erweitert diese um einen Authentisierungsdienst.

Im *Sicheren Netz der KVen* werden den Teilnehmern von den KVen und der KBV Dienste und Anwendungen zur Verfügung gestellt, die mit dem Begriff Applikationen (oder auch KV-Apps) zusammengefasst werden. Es besteht auch für KV-fremde Dienstanbieter die Möglichkeit, Dienste anzubieten, Voraussetzung hierfür ist eine Zertifizierung der betreffenden Applikation durch die KBV.

Der Anschluss mittels KV-SafeNet erfolgt durch einen von der KBV zertifizierten Provider. Dieser stellt einem Teilnehmer alle technischen Voraussetzungen zur Anbindung an das *Sichere Netz der KVen* mittels einer Hardware-VPN-Lösung zur Verfügung und garantiert für die Sicherheit dieser Verbindung. Der Provider stellt dem Teilnehmer hierzu einen KV-SafeNet-Router zur Verfügung.

Beim Anschluss eines Teilnehmers über KV-FlexNet stellt die jeweilige KV des Teilnehmers eine von der KBV zugelassene Software-VPN-Lösung zur Verfügung und garantiert für die Sicherheit der Verbindung.

1.2 Ziel des Dokuments

Die Richtlinie KV-SafeNet (Netzkopplung) beschreibt die Bedingungen für den gesicherten Anschluss von Teilnehmern aus bereits in sich abgesicherten gesundheitsmedizinischen Netzinfrastrukturen an das *Sichere Netz der KVen*.

Hierzu werden eine gesicherte Verbindung zwischen den Teilnehmern der anzubindenden Netzinfrastruktur, dem Provider sowie der KV und zudem die Bedingungen für die Zertifizierung eines Providers beschrieben. Die gesicherte Verbindung basiert auf der sicheren Hardware-VPN-Lösung KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] und erweitert diese um einen Authentisierungsdienst sowie um die hierfür notwendigen regulatorischen Maßnahmen. Diese Richtlinie bildet die Grundlage für die Zertifizierung von Providern.

1.3 Klassifizierung und Adressaten des Dokuments

Dieses Dokument ist öffentlich zu verwenden. Es richtet sich an alle am *Sicheren Netz der KVen* beteiligten Akteure, insbesondere an bereits zertifizierte KV-SafeNet-Provider, die sich zusätzlich für die Durchführung von Netzkopplungen zertifizieren lassen möchten.

* Disclaimer: Bitte beachten Sie, dass KV-SafeNet nicht mit der Firma SafeNet, Inc., USA, in firmenmäßiger oder vertraglicher Verbindung steht.
[1] In der jeweiligen KV kann diese Lösung auch einen anderen Namen haben.

2 Gültigkeit, Anwendungsbereich und Abgrenzung

Die Richtlinie KV-SafeNet (Netzkopplung) ist gültig für den Anschluss von Teilnehmern aus anderen, bereits in sich abgesicherten Netzinfrastrukturen des gesundheitsmedizinischen Betriebs der Bundesrepublik Deutschland, z.B. für den Anschluss verschiedener Teilnetze und einzelner oder mehrerer Standorte einer Organisation an das *Sichere Netz der KVen*.

Diese Fassung der Richtlinie KV-SafeNet (Netzkopplung) ist ausschließlich gültig und zwingend anzuwenden für den Anschluss von berechtigten Teilnehmern aus Krankenhäusern und Krankenhaus- bzw. Klinikketten an das *Sichere Netz der KVen*.

Diese Richtlinie ist nicht gültig und nicht anzuwenden für den Anschluss von Teilnehmern aus dem Internet, aus Netzwerken außerhalb des gesundheitsmedizinischen Betriebs oder für die Anbindung von KV-WebNet-Teilnehmern einzelner KVen an das *Sichere Netz der KVen*.

Mit Inkrafttreten dieses Dokumentes ist ein Anschluss großer Netzinfrastrukturen ausschließlich nach den Maßgaben dieser Richtlinie zulässig.

Bereits bestehende Anschlüsse großer Netzinfrastrukturen sollten unverzüglich konform zur Richtlinie KV-SafeNet (Netzkopplung) umgestellt werden, müssen jedoch grundsätzlich bis 31.12.2012 umgestellt sein.

3 Anwendung der Richtlinie KV-SafeNet

Grundsätzlich gelten alle Regelungen und damit alle Abschnitte der zum Zeitpunkt der Zertifizierung geltenden Fassung der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] für die Richtlinie KV-SafeNet (Netzkopplung) und sind entsprechend umzusetzen. Notwendige Ergänzungen oder Abweichungen für den Anwendungsbereich der Netzkopplung werden in dieser Richtlinie definiert.

4 Grundlegendes Vorgehen und Verantwortlichkeiten

In diesem Kapitel wird das grundlegende Vorgehen bei der Durchführung der Netzkopplung umrissen, welches im Anschluss detailliert wird.

Unter Netzkopplung wird der Anschluss von Teilnehmern aus bereits in sich abgesicherten größeren gesundheitsmedizinischen Netzinfrastrukturen an das *Sichere Netz der KVen* verstanden. Ein durch die KBV zertifizierter Provider stellt dem Betreiber der angeschlossenen Netzinfrastruktur alle technischen Voraussetzungen zur Anbindung an das *Sichere Netz der KVen* bereit. Die Anbindung erfolgt mittels einer auf der Anbindungsvariante KV-SafeNet basierenden Hardware-VPN-Lösung. Der Provider stellt dem Betreiber der anzuschließenden Netzinfrastruktur hierzu einen Netzkopplungsrouter zur Verfügung. Jeder Teilnehmer muss sich vor dem Zugang zum *Sicheren Netz der KVen* mit einer persönlichen Kennung am Netzkopplungsrouter authentisieren.

Mit dem Begriff *Betreiber der angeschlossenen Netzinfrastruktur* ist immer die verantwortliche Institution gemeint, unabhängig davon, ob die Institution den Betrieb selbst durchführt oder diesen an andere Unternehmen ausgelagert hat.

Ein für die Netzkopplung zertifizierter Provider richtet auf Antrag eines Betreibers einer anzuschließenden Netzinfrastruktur eine gesicherte Verbindung zum *Sicheren Netz der KVen* ein, um den Teilnehmern aus der anzuschließenden Netzinfrastruktur Zugang zu den dort bereitgestellten Applikationen zu ermöglichen.

Im Rahmen der Netzkopplung muss die KV, in deren Gebiet der Anschluss erfolgen soll, gegenüber dem Provider die Zulassung des Anschlusses des Betreibers einer Netzinfrastruktur an das *Sichere Netz der KVen* bestätigen und spricht damit eine Genehmigung für die Organisationseinheit aus.

Der Betreiber einer anzuschließenden Netzinfrastruktur schließt mit dem Provider einen Vertrag, der den in seinem Netz befindlichen Teilnehmern einen Zugang zum *Sicheren Netz der KVen* ermöglicht.

Der Netzkopplungsrouter stellt die Funktionalität eines KV-SafeNet-Routers sowie einen Authentisierungsdienst bereit. Zusätzlich zur Routing-Funktionalität ermöglicht der Netzkopplungsrouter damit die eindeutige Identifizierung und personenbezogene Authentisierung der Teilnehmer.

Der Betreiber einer anzuschließenden Netzinfrastruktur benennt dem Provider die Teilnehmer, die Zugang zum *Sicheren Netz der KVen* erhalten sollen. Der Provider ermöglicht diesen berechtigten Teilnehmern den Zugang zum *Sicheren Netz der KVen*. Der Provider teilt allen betreffenden KVen mit, welche Teilnehmer aus dem entsprechenden KV-Gebiet eingerichtet werden. Die KBV/KVen haben hierbei ein rückwirkendes Einsichtnahme- und Vetorecht für einzelne Teilnehmer.

Die Teilnehmer müssen sich bei jedem Zugang zum *Sicheren Netz der KVen* am Netzkopplungsrouter mit einer persönlichen Teilnehmerkennung (z.B. Nutzername und Passwort) authentisieren. Eine eindeutige Identifikation des Teilnehmers durch den Netzkopplungsrouter muss sichergestellt werden.

5 Zertifikat

Das Zertifikat bescheinigt dem Provider, dass seine Anbindung den Bestimmungen dieser Richtlinie genügt.

Die in den folgenden Abschnitten definierten Anforderungen müssen für die Erlangung und die Aufrechterhaltung des Zertifikates zur Durchführung der Netzkopplung erfüllt sein.

Die in der aktuell gültigen Version der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] definierten Regelungen betreffend KV-SafeNet-Zertifizierung, insbesondere

- Überprüfung [KBV_SNK_LFEX_Überprüfung_Provider]
- Bereitstellung der Hardware,
- Änderung der Zugangskomponenten,
- Einzureichende Unterlagen,
- Änderungen der Richtlinie,
- Rezertifizierung,
- Entzug des Zertifikats und
- Haftungsausschluss der Kassenärztlichen Vereinigungen und der KBV

sind auch entsprechend für die Zertifizierung zur Durchführung der Netzkopplung anzuwenden.

Notwendige Ergänzungen oder Abweichungen für den Anwendungsbereich der Netzkopplung werden nachfolgend definiert.

5.1 Voraussetzungen für die Zertifizierung

Voraussetzung für die Erlangung des Zertifikates zur Durchführung der Netzkopplung ist ein gültiges Zertifikat des Providers entsprechend Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet].

5.2 Zertifizierung

Mit dem Antrag auf eine Zertifizierung verpflichtet sich der Provider zur Einhaltung der Maßgaben dieser Richtlinie. Die Zertifizierung erfolgt durch die KBV anhand des Dokuments [KBV_SNK_LFEX_Zert_Netzkopplung]. Die Kosten der Zertifizierung trägt der Provider. Die Zertifizierung des Providers wird von allen, am *Sicheren Netz der KVen* beteiligten KVen, anerkannt. Ausschließlich zertifizierte Provider erhalten die Möglichkeit zur Anbindung von Teilnehmern an das *Sichere Netz der KVen* und können die Anbindung einer anzuschließenden Netzinfrastruktur realisieren.

Für die Zertifizierung zur Durchführung der Netzkopplung wird die zum Zeitpunkt der Zertifizierung geltende Fassung der Richtlinie KV-SafeNet zugrunde gelegt und nicht die Fassung, nach der der Provider seine KV-SafeNet-Zertifizierung erlangt hat.

Die gleichzeitige Antragstellung zur Zertifizierung von KV-SafeNet und zur Zertifizierung der Netzkopplung ist möglich.

5.3 Bereitstellung der Hardware

Der Provider stellt der KBV zu Zertifizierungszwecken je einen als Netzkopplungsrouter einzusetzenden Gerätetyp zur Verfügung.

Der Provider ist verpflichtet, die notwendigen Maßnahmen zu ergreifen, um zu Überprüfungszwecken innerhalb von zehn Werktagen jeden zertifizierten und im Einsatz befindlichen Gerätetyp der KBV im vollständig konfigurierten Zustand zur Verfügung zu stellen.

Abweichend von den Regelungen der zum Zeitpunkt der Zertifizierung gültigen Version der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] verbleibt für die Laufzeit des Zertifikates kein Gerät bei der KBV.

5.4 Zertifikatslaufzeit

Das Zertifikat zur Bereitstellung der Netzkopplung ist an die Laufzeit des zugrundeliegenden KV-SafeNet-Zertifikats gebunden. Es erlischt, wenn das als Voraussetzung dieser Zertifizierung zugrunde liegende KV-SafeNet-Zertifikat erloschen ist.

5.5 Zulassungsfähige Lösungen

In Abhängigkeit von den zu nutzenden Anwendungen und von der IT-Infrastruktur des Betreibers der anzuschließenden Netzinfrastruktur sind verschiedene Lösungskonzepte jeweils separat zulassungsfähig.

Der Provider erhält die Zertifizierung ausschließlich für das eingereichte Konzept und die darin spezifizierte Lösung. Der Provider muss mindestens die in 7.1 „Basisanforderungen“ definierten Regelungen umsetzen und kann ergänzend die in 7.2 „Optionale Anforderungen“ definierten Regelungen umsetzen.

Das Zertifikat berechtigt den Provider zum Anschluss von Betreibern von Netzinfrastrukturen ausschließlich mittels des zugelassenen Konzeptes.

6 Anforderungen an den Netzkopplungsvertrag

Diese Richtlinie ist Vertragsgrundlage zwischen Provider und Betreiber der anzuschließenden Netzinfrastruktur.

Der Provider verpflichtet sich, ausschließlich das im Rahmen der Zertifizierung eingereichte Muster als Netzkopplungsvertrag zu verwenden.

Die in den folgenden Abschnitten definierten Anforderungen müssen im Netzkopplungsvertrag berücksichtigt sein.

Die Regelungen der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] bezüglich des Teilnehmervertrages beziehen sich auf das zwischen Teilnehmer und Provider geschlossene Vertragsverhältnis. Diese Regelungen sind äquivalent auf den zwischen Betreiber der anzubindenden Netzinfrastruktur und Provider zu schließenden Netzkopplungsvertrag umzusetzen.

Die in der aktuellen Version der Richtlinie KV-SafeNet definierten Regelungen betreffend des Teilnehmervertrages, insbesondere

- Außerordentliche Kündigung,
- Beendigung des Vertragsverhältnisses,
- Transparenz des Angebotes,
- Bereitstellungszeitraum des Zugangs,
- Teilnehmersupport des Anbieters,
- Servicezeiten und
- Vertragsstrafe

sind daher entsprechend im Netzkopplungsvertrag zu berücksichtigen.

Notwendige Ergänzungen oder Abweichungen für den Anwendungsbereich der Netzkopplung werden in den folgenden Abschnitten definiert.

6.1 Vertragspartner

Vertragspartner des Providers bei der Leistungserbringung ist ausschließlich der Betreiber der anzuschließenden Netzinfrastruktur.

Teilnehmer und Provider gehen kein Vertragsverhältnis ein.

6.2 Vertragsvoraussetzung

Voraussetzung für die Wirksamkeit des Vertrags zwischen dem Betreiber der anzuschließenden Netzinfrastruktur und dem Provider ist die Zulassung des Betreibers der anzuschließenden Netzinfrastruktur als Organisationseinheit zum *Sicheren Netz der KVen* durch die jeweils zuständige KV. Die zuständige KV ist die, in deren Gebiet der Anschluss an das *Sichere Netz der KVen* erfolgen soll. Im Allgemeinen ist das die KV, in deren Gebiet sich der Netzkopplungsrouter des Betreibers der anzuschließenden Netzinfrastruktur befindet.

Im Speziellen kann die Zulassung eines Betreibers einer anzuschließenden Netzinfrastruktur auch durch die KBV in Abstimmung mit den KVen erfolgen, falls dieser von bundesweiter Bedeutung ist.

Der Provider muss im Rahmen des Vertrages den Vertragspartner über sein Zertifikat und die entsprechende Zertifikatslaufzeit informieren.

6.3 Vertragsverlängerung

Vor einer Vertragsverlängerung muss sich der Provider bei der jeweils zuständigen KV die Gültigkeit der Zulassung des Betreibers der angeschlossenen Netzinfrastruktur zum *Sicheren Netz der KVen* bestätigen lassen.

6.4 Kontrollrecht des Betreibers der anzuschließenden Netzinfrastruktur

Die bezüglich Kontrollrecht eines Teilnehmers definierten Regelungen der zum Zeitpunkt der Zertifizierung gültigen Version der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] gelten entsprechend im Rahmen der Richtlinie KV-SafeNet (Netzkopplung) für den Betreiber der anzuschließenden Netzinfrastruktur.

6.5 Nutzung des Zugangs zum *Sicheren Netz der KVen*

Teilnehmer aus der angeschlossenen Netzinfrastruktur erhalten einen zweckgebundenen Zugang zum *Sicheren Netz der KVen* und den dort angebotenen Diensten.

Es ist dem Betreiber der angeschlossenen Netzinfrastruktur untersagt, den KV-Backbone zur internen Vernetzung oder zur Vernetzung mit weiteren Netzinfrastrukturen anderer Organisationen zu nutzen.

Der Vertrag zwischen dem Betreiber der anzuschließenden Netzinfrastruktur und dem Provider muss eine diesbezügliche Regelung beinhalten.

6.6 Benennung der berechtigten Teilnehmer

Der Betreiber der anzuschließenden Netzinfrastruktur benennt dem Provider die berechtigten Teilnehmer seiner Organisationseinheit und haftet für die Richtigkeit der Angaben. Die Benennung erfolgt mit folgenden Pflichtangaben

- Nutzername
- Nachname und Vorname des Teilnehmers
- Gebiet der KV-Zugehörigkeit des Teilnehmers
- Lebenslange Arztnummer (LANR) des Teilnehmers, falls der Teilnehmer eine LANR besitzt
- Betriebsstättennummer (BSNR) des Teilnehmers, falls der Teilnehmer eine BSNR besitz

Berechtigte Teilnehmer sind die Mitglieder der Kassenärztlichen Vereinigungen, also Vertragsärzte und –psychotherapeuten, sowie ggf. Teilnehmer, die Dienste der KVen nutzen möchten.

Teilnehmer können nur natürliche Personen sein, Gruppenberechtigungen sind nicht zulässig.

Der Provider gewährt ausschließlich den benannten berechtigten Teilnehmern Zugang zum *Sicheren Netz der KVen*, eine explizite Bestätigung einzelner Teilnehmer durch KVen ist nicht notwendig.

Der Betreiber der anzuschließenden Netzinfrastruktur muss Änderungen der benannten Teilnehmer, z.B. wegen Kündigung des Arbeitsverhältnisses eines Teilnehmers, unverzüglich dem Provider mitteilen, der diese Änderungen wiederum unverzüglich umsetzen muss.

Der Vertrag zwischen dem Betreiber der anzuschließenden Netzinfrastruktur und dem Provider muss eine diesbezügliche Regelung beinhalten.

6.7 Kontrollrecht und Vorbehalt der KVen/KBV bezüglich der Teilnehmer

Die KVen haben die Pflicht, den Teilnehmerkreis zu kontrollieren und zu bestimmen.

Hierzu teilt der Provider allen betreffenden KVen mit, welche Teilnehmer aus dem jeweiligen KV-Gebiet auf dem Netzkopplungsrouter eingerichtet werden. Die KVen können innerhalb der Frist von drei Arbeitstagen ein Vetorecht für einzelne Teilnehmer ausüben, nach Ablauf der Frist richtet der Provider die Teilnehmerberechtigungen auf dem Netzkopplungsrouter ein.

Weiterhin behalten sich die KVen und die KBV das Recht vor, Einsicht in die auf dem Netzkopplungsrouter eingerichteten Teilnehmer zu bekommen und ggf. auch zu einem späteren Zeitpunkt ein Vetorecht gegenüber einzelnen Teilnehmern auszuüben. Der Provider muss die betroffenen Teilnehmer unverzüglich deaktivieren.

Der Vertrag zwischen dem Betreiber der anzuschließenden Netzinfrastruktur und dem Provider muss eine entsprechende Klausel zu Einsichtnahme- und Vetorecht beinhalten.

6.8 Authentisierung der Teilnehmer für den Zugang zum *Sicheren Netz der KVen*

Der Zugang eines Teilnehmers zum *Sicheren Netz der KVen* wird durch eine Authentisierung des Teilnehmers am Netzkopplungsrouter abgesichert. Nur erfolgreich authentisierte Teilnehmer erhalten Zugang zum *Sicheren Netz der KVen*.

Jeder berechtigte Teilnehmer erhält hierzu eine persönliche Teilnehmerkennung. Diese Teilnehmerkennungen dürfen nicht an andere Teilnehmer weitergegeben oder anderweitig missbraucht werden.

Die Teilnehmerkennungen werden ausschließlich vom Provider eingerichtet und gepflegt, der Betreiber der anzuschließenden Netzinfrastruktur hat keinen Zugriff auf die Teilnehmerkennungen.

Der Vertrag zwischen dem Betreiber der anzuschließenden Netzinfrastruktur und dem Provider muss eine diesbezügliche Regelung beinhalten.

6.9 Protokollierung der Teilnehmerzugriffe

Teilnehmerzugriffe auf das *Sichere Netz der KVen* sind im rechtmäßigen Rahmen zu protokollieren. Änderungen der gesetzlichen Vorgaben müssen vom Provider unverzüglich umgesetzt werden.

Der Vertrag zwischen dem Betreiber der anzuschließenden Netzinfrastruktur und dem Provider muss eine diesbezügliche Regelung beinhalten.

6.10 Pflichten des Betreibers der anzuschließenden Netzinfrastruktur und der darin befindlichen Teilnehmer

Aufgrund des erhöhten Sicherheitsbedarfs beim Anschluss von Teilnehmern an das *Sichere Netz der KVen* müssen an den Betreiber der anzubindenden Infrastruktur bezüglich der PC-Arbeitsplätze, der Netzinfrastruktur und auch organisatorisch besondere Ansprüche gestellt werden.

Der Betreiber der angeschlossenen Netzinfrastruktur muss eine dem Stand der Technik entsprechende Umsetzung gewährleisten und die geltenden Datenschutz- und Datensicherheitsempfehlungen bzw. Vorgaben einhalten. Der Stand der Technik wird durch die aktuellen Maßnahmen des BSI im Rahmen der Grundschutzkataloge definiert.

Der Betreiber der anzuschließenden Netzinfrastruktur verpflichtet sich gegenüber dem Provider zur Einhaltung der Regelungen dieses Abschnittes 6.10 und kann bei Missbrauch haftbar gemacht werden.

Der Betreiber der anzuschließenden Netzinfrastruktur muss die Kenntnisnahme der in diesem Abschnitt festgelegten Sicherheitshinweise schriftlich im Vertrag bestätigen. Weiterhin muss er bestätigen, dass die über seine Netzinfrastruktur angeschlossenen Teilnehmer die Sicherheitshinweise zur Kenntnis genommen haben bzw. zur Kenntnis nehmen werden, sobald die Anbindung der Teilnehmer erfolgt.

Der Vertrag zwischen dem Betreiber der anzuschließenden Netzinfrastruktur und dem Provider muss diesbezügliche Regelungen beinhalten.

6.10.1 PC-Arbeitsplätze

Die im veröffentlichten Merkblatt „Sicherheitsanforderungen für KV-SafeNet-Arbeitsplätze“ [KBV_SNK_MBEX_Sicherheit_Arbeitsplätze] beschriebenen Maßnahmen sind äquivalent umzusetzen.

Insbesondere sind die PC-Arbeitsplätze, von denen aus die Teilnehmer Zugang zum *Sicheren Netz der KVen* erhalten können, folgendermaßen durch den Betreiber der anzubindenden Netzinfrastruktur bereitzustellen bzw. zu konfigurieren:

- Der PC-Arbeitsplatz soll dem aktuellen Stand der Technik entsprechen und insbesondere aktuelle Versionen von Betriebssystemen, Antiviren-Software, Anti-Malware und Firewall enthalten und entsprechend sicher konfiguriert sein.
- Die Arbeit an dem PC-Arbeitsplatz erfordert eine Anmeldung des Teilnehmers am PC, der Zugriff von unbefugten Personen auf den PC-Arbeitsplatz ist durch ein Benutzer- und Rollenkonzept zu verhindern.
- Grundsätzliche Administrationsrichtlinien insbesondere im Bereich der Benutzerberechtigungen für die PC-Arbeitsplätze sind einzuhalten, entsprechend der BSI Maßnahme M 2.38[2] (Aufteilung der Administrationstätigkeiten).
- Bei Inaktivität wird eine automatische Sperre des PC-Arbeitsplatzes mit anschließend erforderlicher Anmeldung zum Aufheben der Sperre vorgenommen.
- Der PC-Arbeitsplatz darf keine direkte Verbindung mit dem Internet haben. Eine Verbindung des PC-Arbeitsplatzes mit dem Internet über die Netzinfrastruktur des Betreibers ist erlaubt.
- Die Räumlichkeiten des PC-Arbeitsplatzes müssen so gestaltet sein, dass unbefugte Personen keinen Zugriff auf den Arbeitsplatz erlangen können.

[2] BSI-Maßnahme M 2.38 im Rahmen der Grundschutzkataloge siehe: https://www.bsi.bund.de.

6.10.2 Netzinfrastruktur

Für den Datenschutz und die Datensicherheit in der angeschlossenen Netzinfrastruktur ist der Betreiber der angeschlossenen Netzinfrastruktur voll verantwortlich.

In der angeschlossenen Netzinfrastruktur empfiehlt es sich, folgende Maßnahmen umzusetzen:

- Regelmäßiger Einsatz von Programmen, die Integritätsverletzungen an Programmen und Dateien feststellen können
- Einsatz von Programmen zur Erkennung von Angriffen auf ein IT-System, z.B. ein Intrusion Detection System (IDS) oder ein anderes zur Frühwarnung taugliches Netzüberwachungssystem
- Benutzung aller vorhandenen und rechtmäßigen Protokollmechanismen

Es muss technisch und organisatorisch sichergestellt werden, dass ausschließlich Personen aus der Organisation bzw. Institution des Betreibers der anzuschließenden Netzinfrastruktur Zugang zum Netzkopplungsrouter erlangen können. Personen außerhalb der Organisation, z.B. aus anderen angeschlossenen Netzinfrastrukturen, dürfen keinen Zugang zum Netzkopplungsrouter erhalten.
Das erfolgt mittels einer Zugriffssteuerungsliste (Access Control List) auf dem Netzkopplungsrouter. Der Betreiber der angeschlossenen Netzinfrastruktur benennt dem Provider die erlaubten Netzwerke bzw. Netzbereiche, der Provider richtet die Regeln entsprechend im Netzkopplungsrouter ein.

6.10.3 Organisatorisches

Der Betreiber der anzuschließenden Netzinfrastruktur muss die Teilnehmer über folgende Pflichten des Teilnehmers informieren.

- Die Regelungen der BSI Maßnahme M 2.37[3] (Der aufgeräumte Arbeitsplatz) sind einzuhalten.
- Bei Verlassen des PC-Arbeitsplatzes muss sich der Teilnehmer abmelden.
- Der Teilnehmer darf die ihm zugewiesene persönliche Kennung keinesfalls an andere Personen weitergeben.
- Der Teilnehmer darf ausschließlich seine eigene persönliche Kennung für den Zugang zum *Sicheren Netz der KVen* benutzen.

6.11 Haftungsausschluss

Bezüglich Haftungsausschluss gelten die entsprechenden Regelungen der jeweils aktuellen, zum Zeitpunkt der Zertifizierung gültigen Version der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet].

Ergänzend dazu übernimmt die KV/KBV keinerlei Haftung bezüglich der Sicherheit der anzuschließenden Netzinfrastruktur und der Sicherheit der Arbeitsplätze innerhalb der anzuschließenden Netzinfrastruktur.

[3] BSI-Maßnahme M 2.37 im Rahmen der Grundschutzkataloge siehe: https://www.bsi.bund.de.

6.12 Vorbehalt der KV/KBV bezüglich Missbrauch der Anbindung

Die KV/KBV behält sich das Recht vor, bei Missbrauch der Anbindung des Betreibers der angeschlossenen Netzinfrastruktur oder bei Missbrauch der Anbindung durch einzelne Teilnehmer innerhalb der angeschlossenen Netzinfrastruktur die Anbindung des Netzes oder einzelner Teilnehmer jederzeit zu unterbrechen bzw. durch den Provider unterbrechen zu lassen, um Schaden an Daten, Anwendungen oder angeschlossenen Systemen zu vermeiden.

Der Betreiber der anzuschließenden Netzinfrastruktur und der Provider liefern im Falle eines Missbrauchs auf Anforderung die entsprechenden Verbindungs- und Protokolldaten an die KV/KBV.

Der Vertrag zwischen dem Betreiber der anzuschließenden Netzinfrastruktur und dem Provider muss diesbezügliche Regelungen beinhalten.

6.13 Datenschutz

Der Vertrag muss einen Hinweis auf den Datenschutz und eine Beschreibung der notwendigen Sicherheitsmaßnahmen in der anzuschließenden Netzinfrastruktur und den angeschlossenen Rechnern beinhalten.

6.14 Verfügbarkeit

Der Vertrag zwischen dem Betreiber der anzuschließenden Netzinfrastruktur und dem Provider muss eine Regelung beinhalten, die die Verfügbarkeit der Anbindung der anzuschließenden Netzinfrastruktur an das *Sichere Netz der KVen* definiert.

6.15 Aufstellung und physikalische Absicherung des Netzkopplungsrouters

Der Netzkopplungsrouter bzw. die einzelnen Komponenten des Netzkopplungsrouters werden vom Provider bereitgestellt.

Die einzelnen Komponenten des Netzkopplungsrouters müssen physikalisch gegen unbefugten Zugang gesichert werden, z.B. durch Aufbewahrung in einem gesicherten Rechenzentrum.

Der Vertrag zwischen dem Betreiber der anzuschließenden Netzinfrastruktur und dem Provider muss diesbezügliche Regelungen beinhalten.

7 Technische Anforderungen an den Provider

Die in der aktuell gültigen Version Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] definierten Regelungen betreffend den technischen Anforderungen an den Provider, insbesondere

- Nutzung des KV-Backbones,
- Einschränkung der Nutzung,
- Deaktivierung ungenutzter Ports,
- Routing,
- DNS,
- Sichtbarkeit,
- Sicherheit der Zugangsdaten,
- Überwachungsmaßnahmen des Providers und
- Betriebszeit und Verfügbarkeit

sind entsprechend für die Richtlinie KV-SafeNet (Netzkopplung) gültig.

Notwendige Ergänzungen oder Abweichungen für den Anwendungsbereich der Netzkopplung werden in diesem Abschnitt definiert.

7.1 Basisanforderungen

7.1.1 VPN-Konzentrator

Bezüglich der Konzentratoren gelten die entsprechenden Regelungen der jeweils aktuellen, zum Zeitpunkt der Zertifizierung gültigen Version der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet].

Bereits im Rahmen einer Zertifizierung nach Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] installierte Konzentratoren dürfen zur Durchführung der Netzkopplung genutzt werden.

7.1.2 Netzkopplungsrouter

Der Netzkopplungsrouter besteht technisch aus der Router-Komponente und einer Authentisierungs-Komponente. Wenn im Folgenden von Netzkopplungsrouter die Rede ist, ist immer die gesamte Konstruktion gemeint.

Der Netzkopplungsrouter wird vom Provider bereitgestellt. Falls sich der Netzkopplungsrouter aus einzelnen Komponenten zusammensetzt, ist der Provider für die Bereitstellung der einzelnen Komponenten verantwortlich.

Die Gesamtkonstruktion des Netzkopplungsrouters sollte aus Gründen der Wartbarkeit aus möglichst wenigen physischen Komponenten bestehen, die maximale zertifizierungsfähige Obergrenze liegt bei drei Komponenten.

7.1.2.1 Identifizierbarkeit der Zugriffe

Zugriffe auf das *Sichere Netz der KVen* müssen eindeutig identifizierbar sein. Die Identifizierbarkeit muss sowohl auf Ebene des Netzkopplungsrouters als auch auf Ebene der Teilnehmer gewährleistet sein.

Jeder Netzkopplungsrouter muss im *Sicheren Netz der KVen* durch eine eindeutige, feste IP-Adresse adressierbar und identifizierbar sein.

Die Teilnehmer müssen eindeutig anhand persönlicher Merkmale (z.B. einer Teilnehmerkennung) am Netzkopplungsrouter identifizierbar sein.

Das Konzept zur Umsetzung der Anforderung obliegt dem Provider und ist im Rahmen der Zertifizierung vorzulegen.

7.1.2.2 Adressierung des Netzkopplungsrouters

Abweichend von den Regelungen der zum Zeitpunkt der Zertifizierung gültigen Version der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] wird jedem Netzkopplungsrouter eine feste IP-Adresse zugeordnet, die dynamische Adressvergabe ist für Netzkopplungsrouter nicht zulässig.

7.1.2.3 Authentisierung der Teilnehmer

Jeder Zugang eines Teilnehmers zum *Sicheren Netz der KVen* wird durch eine Authentisierung des Teilnehmers am Netzkopplungsrouter abgesichert. Nur erfolgreich authentisierte Teilnehmer erhalten Zugang zum *Sicheren Netz der KVen*. Die Authentisierung ist ausschließlich für den Teilnehmer gültig.

Jeder berechtigte Teilnehmer erhält hierfür eine persönliche Teilnehmerkennung. Teilnehmerkennungen dürfen nicht an andere Teilnehmer weitergegeben oder anderweitig missbraucht werden. Gruppenaccounts sind nicht zulässig.

Für jede Teilnehmerkennung müssen zusätzlich zum Berechtigungsnachweis die im Abschnitt 6.6 „Benennung der berechtigten Teilnehmer“ genannten Attribute im Netzkopplungsrouter eingerichtet werden.

Die Authentisierung eines Teilnehmers muss vor der Übertragung von Nutzdaten erfolgen. Erst nach erfolgreicher Authentisierung eines Teilnehmers erfolgt die Übertragung von Nutzdaten in das *Sichere Netz der KVen*. Die Authentisierung ist für die Dauer der Verbindung gültig, eine nochmalige Authentisierung ist nicht notwendig.

Nach einer Inaktivität von zwei Stunden muss die Verbindung automatisch vom Netzkopplungsrouter beendet werden.

Eine mehrfache gleichzeitige Anmeldung derselben Benutzerkennung ist durch den Verzeichnisdienst zwingend zu unterbinden, ein Teilnehmer kann nur eine aktive Verbindung haben.

Der Provider stellt hierzu einen Authentisierungs- und Verzeichnisdienst bereit, der ausschließlich vom Provider betrieben wird.

Die Teilnehmerkennungen werden ausschließlich durch den Provider eingerichtet, geändert, deaktiviert oder gelöscht.

Der Berechtigungsnachweis (z.B. das Passwort) wird ausschließlich durch den Provider erstmalig erzeugt und kann nur durch den Provider oder durch den jeweiligen Teilnehmer (z.B. bei Änderung des eigenen Passwortes) geändert werden. Die erstmalige Übermittlung des Berechtigungsnachweises an den Teilnehmer muss auf vertraulichem Weg, z.B. verschlüsselte Email, postalisch per Standard-Brief oder persönlich (d.h. nicht telefonisch) erfolgen.

Im Falle der Verwendung von Passwörtern ist nach der ersten Anmeldung am Netzkopplungsrouter eine Änderung des Passwortes durch den Teilnehmer zwingend notwendig.

Der Betreiber der anzuschließenden Netzinfrastruktur hat keinen administrativen Zugang zum Authentisierungs- und Verzeichnisdienst.

Es muss eine anerkannte und sichere Authentisierungs-Lösung eingebunden werden. Diese muss dem Stand der Technik entsprechen und soll der vom BSI herausgegebenen BSI-Maßnahme M 4.133[4] (Geeignete Auswahl von Authentifikationsmechanismen) entnommen

[4] BSI-Maßnahme M 4.133 im Rahmen der Grundschutzkataloge siehe: https://www.bsi.bund.de.

werden. Zugelassene Authentisierungsmechanismen sind Passwörter, Zugangskarten und biometrische Techniken. Eine ergänzende Zwei-Faktor-Authentisierung z.B. mittels Einmalpasswörtern, ist möglich.

Bei Verwendung von Passwörtern sind die Regelungen entsprechend der BSI-Maßnahme M 2.11[5] (Regelung des Passwortgebrauchs) umzusetzen.

Bei einem erfolglosen Authentisierungsversuch darf dem Teilnehmer kein Hinweis darauf gegeben werden, ob die Kennung des Teilnehmers überhaupt im System vorhanden ist. Dem Teilnehmer sollte eine Meldung wie z.B. „Name und/oder Passwort fehlerhaft“ angezeigt werden.

Nach einer vorgegebenen Anzahl erfolgloser Authentisierungsversuche muss die betroffene Benutzerkennung gesperrt werden oder es muss jeder weitere Authentisierungsversuch zeitlich zunehmend verzögert werden.

Die Entsperrung kann entweder durch den Provider erfolgen oder durch den Teilnehmer.

Wenn die Entsperrung durch den Provider vorgenommen wird, muss der Prozess der Erzeugung und Versendung der Berechtigungsnachweise äquivalent zum initialen Prozess durchgeführt werden.

Wenn die Entsperrung durch den Teilnehmer vorgenommen wird, müssen als gesonderter Prozess der Authentisierung weitere Benutzerdaten abgefragt werden. Die abzufragenden Benutzerdaten dürfen nicht allgemein bekannt sein (z.B. Namen des Teilnehmers, Geburtsdatum).

Wiederholte fehlerhafte Passworteingaben für eine Benutzerkennung oder unzulässige Verbindungsversuche können auf einen Missbrauch hindeuten und sollten zu einer unverzüglichen Warnung des Systems an den Provider führen. Die Schwellwerte hierzu sind im Rahmen eines Incident Management Systems des Providers vom Provider selbständig festzulegen und entsprechende Maßnahmen zu treffen.

Änderungen an Benutzerdaten und Berechtigungsnachweisen sind durch den Verzeichnisdienst zwingend zu protokollieren.

7.1.2.4 Protokollierung der Teilnehmerzugänge

Teilnehmerzugänge auf das *Sichere Netz der KVen* sind im rechtmäßigen Rahmen zu protokollieren. Änderungen der gesetzlichen Vorgaben müssen vom Provider unverzüglich umgesetzt werden.

Die folgenden Absätze dieses Abschnittes sind im Rahmen der rechtmäßigen Protokollierung der Teilnehmerzugänge umzusetzen.

Für jeden erfolgreichen Verbindungsaufbau und -abbau und für jeden abgewiesenen Verbindungsaufbau muss eine Protokollierung vorgenommen werden.

Zu protokollieren sind

- das identifizierende Merkmal des Teilnehmers, z.B. die Teilnehmerkennung,
- Datum und Zeit des Verbindungsaufbaus, sowie die Verbindungsdauer,

Die eingesetzten Verfahren zur Protokollierung müssen dem Stand der Technik entsprechen und können der vom BSI herausgegebenen BSI-Maßnahme M 4.476 (Protokollierung der Sicherheitsgateway-Aktivitäten) entnommen werden.

[5] BSI-Maßnahme M 2.11 im Rahmen der Grundschutzkataloge siehe: https://www.bsi.bund.de.
[6] BSI-Maßnahme M 4.47 im Rahmen der Grundschutzkataloge siehe: https://www.bsi.bund.de.

7.1.2.5 Verschlüsselung

Bezüglich Verschlüsselung gelten die entsprechenden Regelungen der jeweils aktuellen, zum Zeitpunkt der Zertifizierung gültigen Version der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] und sind entsprechend auf die Richtlinie KV-SafeNet (Netzkopplung) und den Netzkopplungsrouter anzuwenden.

Die Verbindung zwischen Netzkopplungsrouter und Konzentrator muss durch einen hochwertig verschlüsselten Hardware-VPN Tunnel äquivalent zum KV-SafeNet-Anschluss geschützt sein, es gelten die Regelungen der Richtlinie KV-SafeNet.

Ergänzend gelten folgende Regelungen:

Die von den Teilnehmern übermittelten Daten zur Authentisierung müssen vor einem Zugriff Dritter durch eine Verschlüsselung geschützt sein.

Datenschutz und Datensicherheit der Kommunikation zwischen den einzelnen Komponenten des Netzkopplungsrouters muss dem aktuellen Stand der Technik entsprechen und verschlüsselt sein.

7.1.3 Datendurchleitung und zu unterstützende Protokolle

Der Netzkopplungsrouter muss sicherstellen, dass die zwischen dem Arbeitsplatz-PC und den Anwendungen im *Sicheren Netz der KVen* stattfindende Datenkommunikation mindestens für Webanwendungen mit den Protokollen HTTP und HTTPS unterstützt wird. Eine SSL/TLS-Verschlüsselung zwischen dem Arbeitsplatz-PC und den Anwendungen im *Sicheren Netz der KVen* soll hierbei nicht aufgebrochen werden.

7.1.4 Verhinderung des Zugriffs von nicht berechtigten Netzwerken

Es muss technisch und organisatorisch sichergestellt werden, dass ausschließlich Personen aus der Organisation bzw. Institution des Betreibers der anzuschließenden Netzinfrastruktur Zugang zum Netzkopplungsrouter erlangen können. Personen außerhalb der Organisation, z.B. aus anderen angeschlossenen Netzinfrastrukturen oder außerhalb des Gebietes der Bundesrepublik Deutschland, dürfen keinen Zugang zum Netzkopplungsrouter erhalten.

Das erfolgt mittels einer Zugriffssteuerungsliste (Access Control List) auf dem Netzkopplungsrouter. Der Betreiber der angeschlossenen Netzinfrastruktur benennt dem Provider die erlaubten Netzwerke bzw. Netzbereiche, der Provider richtet die Regeln entsprechend im Netzkopplungsrouter ein.

7.1.5 Unbefugter Zugriff

Die bezüglich unbefugter Zugriffe definierten Regelungen der zum Zeitpunkt der Zertifizierung gültigen Fassung der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] gelten entsprechend auch für die Richtlinie KV-SafeNet (Netzkopplung). Das in der Richtlinie KV-SafeNet definierte Teilnehmernetz entspricht im Rahmen der Netzkopplung der angeschlossenen Netzinfrastruktur, die Regelungen sind äquivalent umzusetzen.

7.1.6 Betrieb und Standort des Netzkopplungsrouters

Der Netzkopplungsrouter bzw. die einzelnen Komponenten des Netzkopplungsrouters dürfen ausschließlich durch den Provider betrieben werden.

Die Routing-Komponente darf ausschließlich innerhalb der angeschlossenen Netzinfrastruktur betrieben werden.

Der Authentisierungs- und Verzeichnisdienst darf betrieben werden

- innerhalb der angeschlossenen Netzinfrastruktur als separate Komponente
- innerhalb der angeschlossenen Netzinfrastruktur als gemeinsame Komponente mit der Routing-Komponente
- als separate Komponente im Providernetz

Der Authentisierungs- und Verzeichnisdienst darf nicht innerhalb des KV-Backbones, dem Transfernetz oder dem Dienstenetz betrieben werden.

Der Authentisierungs- und Verzeichnisdienst kann für jede angeschlossene Netzinfrastruktur separat oder zentral betrieben werden.

In jedem Fall hat der Provider sicherzustellen, dass die Kennungen der Teilnehmer einer angeschlossenen Netzinfrastruktur gegen Zugriffe von nicht berechtigten Teilnehmern aus anderen angeschlossenen Netzinfrastrukturen abgesichert sind.

7.2 Optionale Anforderungen

Ein zur Zertifizierung eingereichtes Konzept muss mindestens die Basisanforderungen des Abschnitts 7.1 erfüllen.
In Abhängigkeit von den zu nutzenden Anwendungen und von der IT-Infrastruktur des Betreibers der anzuschließenden Netzinfrastruktur sind verschiedene Lösungskonzepte separat zertifizierungsfähig. Dieser Abschnitt beschreibt spezifische Anforderungen, die in Abhängigkeit von den zu nutzenden Anwendungen und der IT-Infrastruktur des Betreibers der anzuschließenden Netzinfrastruktur optional umzusetzen sind.

7.2.1 Datendurchleitung und zu unterstützende Protokolle

Zusätzlich zu den in den Basisanforderungen definierten und zwingend zu unterstützenden Protokollen kann der Netzkopplungsrouter weitere Protokolle unterstützen, z.B. FTP, SMTP, Pop3, IMAP usw. oder auch proprietäre Protokolle spezifischer Anwendungen mit auf dem Arbeitsplatz-PC installierten Client-Komponenten.
Die Datendurchleitung ist aus Teilnehmer- und Applikationssicht transparent.

7.2.2 Terminalserver-Umgebungen

Im Falle des Einsatzes von Multi-User-Umgebungen (z.B. Terminalserver) auf Seiten des Betreibers der anzuschließenden Netzinfrastruktur muss das zur Zertifizierung eingereichte Konzept zwingend sicherstellen, dass Teilnehmer auf Basis von Teilnehmersitzungen und nicht ausschließlich auf Basis von IP-Adressen am Netzkopplungsrouter authentisiert werden.

8 Organisatorische Anforderungen an den Provider

Die in der aktuell gültigen Version Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] definierten Regelungen betreffend der organisatorischen Anforderungen an den Provider, insbesondere

- Mindestumfang des Angebotes,
- Transparenz des Angebotes,
- Installation und Betrieb,
- Support und Wartung,
- Ausschluss des Supports durch die KV/KBV,
- Sicherheit der Zugangsdaten,
- Teststellungen der angebotenen Anbindungsvarianten,
- Missbrauch der Anbindung und
- Vorbehalt bei übermäßiger Belastung des KV-Backbones

sind entsprechend für die Richtlinie KV-SafeNet (Netzkopplung) gültig.

Notwendige Ergänzungen oder Abweichungen für den Anwendungsbereich der Netzkopplung werden in den folgenden Abschnitten definiert.

8.1 Wartungsarbeiten

Die bezüglich Wartungsarbeiten definierten Regelungen der zum Zeitpunkt der Zertifizierung gültigen Fassung der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] gelten entsprechend auch für die Richtlinie KV-SafeNet (Netzkopplung). Das in der Richtlinie KV-SafeNet definierte Vorgehen zwischen Teilnehmer und Provider ist im Rahmen der Netzkopplung äquivalent zwischen dem Betreiber der angeschlossenen Netzinfrastruktur und dem Provider anzuwenden. Die Teilnehmer aus der angeschlossenen Netzinfrastruktur sind durch den Betreiber der angeschlossenen Netzinfrastruktur über Wartungsarbeiten in Kenntnis zu setzen.

8.2 Schutz der Anbindung

Die bezüglich des Schutzes der Anbindung definierten Regelungen der zum Zeitpunkt der Zertifizierung gültigen Version der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] gelten entsprechend auch für die Richtlinie KV-SafeNet (Netzkopplung).

Ergänzend dazu gelten im Rahmen der Netzkopplung folgende Regelungen:

Bei Angriffsversuchen oder sonstigen Sicherheitsvorfällen, die durch den Teilnehmer, den Betreiber der angeschlossenen Netzinfrastruktur, die KBV oder eine KV festgestellt und gemeldet werden, ist der Provider verpflichtet durch geeignete Maßnahmen den Angreifer ausfindig zu machen und angemessene Gegenmaßnahmen einzuleiten.

Angemessene Gegenmaßnahmen bei Missbrauch, festgestellten Angriffsversuchen oder sonstigen Sicherheitsvorfällen, die durch einen Teilnehmer verursacht worden sind, müssen mindestens Folgendes einschließen:

- Deaktivierung des Teilnehmers im Netzkopplungsrouter.
- Meldung des Vorfalls an die KBV. Die KBV informiert andere Provider über den Vorfall, sodass ggf. der Teilnehmer auch in anderen Netzkopplungsroutern anderer Provider deaktiviert werden kann.
- Unterstützung bei der Untersuchung der Aktivitäten des Teilnehmers und der Schadensanalyse z.B. durch Bereitstellung von Log-Dateien.

Angemessene Gegenmaßnahmen bei Missbrauch, festgestellten Angriffsversuchen oder sonstigen Sicherheitsfällen, die durch den Betreiber der angeschlossenen Netzinfrastruktur verursacht worden sind, müssen Folgendes einschließen:

- Deaktivierung der Anbindung des Betreibers der angeschlossenen Netzinfrastruktur und damit aller darüber angeschlossenen Teilnehmer.
- Meldung des Vorfalls an die KBV.
- Unterstützung bei der Schadensanalyse, z.B. durch Bereitstellung von Log-Dateien.

9 Berichtswesen

Die in der aktuell gültigen Version Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] definierten Regelungen betreffend des Berichtswesens, insbesondere

- Technische Berichte und Vorfälle

sind entsprechend für die Richtlinie KV-SafeNet (Netzkopplung) gültig.

Notwendige Ergänzungen oder Abweichungen für den Anwendungsbereich der Netzkopplung werden in diesem Kapitel definiert.

9.1 Vertragsstatistiken

Der Provider hat der für den jeweiligen Betreiber der angeschlossenen Netzinfrastruktur zuständigen KVen folgende Informationen zur Verfügung zu stellen:

- eine Kopie des wirksamen Vertrags (innerhalb von 5 Werktagen nach Vertragswirksamkeit)
- das Datum des Anschlusses
- ggf. das Datum der Kündigung
- ggf. Vertragsänderungen

Der Provider stellt der KBV die aktuellen Preise und Leistungen zur Verfügung und erklärt sich mit der Veröffentlichung der Daten einverstanden. Der KBV steht es frei, die regulären Preislisten aller Provider zu veröffentlichen.

Bei Änderungen der Preise oder Leistungen stellt der Provider der KBV die neuen Preise oder geänderten Leistungen unaufgefordert und unverzüglich zur Verfügung.

9.2 Statistiken über den Datendurchsatz

Der Provider protokolliert den Datendurchsatz der einzelnen Netzkopplungsrouter und stellt diese Übersicht monatlich der KBV bereit.

Diese Angaben erfolgen jeweils pro Netzkopplungsrouter mit dem Datendurchsatz in MByte.

Das Datenformat zur Übermittlung der Statistiken ist in Anhang A dieser Richtlinie definiert.

9.3 Teilnehmerstatistiken für die KBV

Der Provider hat der KBV eine monatliche Teilnehmerstatistik spätestens innerhalb der ersten Woche des Folgemonats bereitzustellen. Folgende Informationen sind dabei durch den Provider zu übermitteln:

- Bezeichnung des Betreibers der angeschlossenen Netzinfrastruktur
- Eingesetzter Typ des Netzkopplungsrouters
- Anzahl der Teilnehmer pro angeschlossener Netzinfrastruktur und Typ des Netzkopplungsrouters

Das Datenformat zur Übermittlung der Statistiken ist in der Anlage A verbindlich definiert.

9.4 Teilnehmerübersichten

Um das in dieser Richtlinie definierte Verfahren der Teilnehmerzulassung zum *Sicheren Netz der KVen* durchführen zu können, muss der Provider alle Teilnehmer an die KVen melden, und zwar sowohl bei der erstmaligen Einrichtung der Teilnehmer und anschließend unverzüglich bei jeder Änderung oder Erweiterung des Teilnehmerkreises. Die KVen können ein Vetorecht gegenüber einzelnen Teilnehmern ausüben.

Der Provider stellt hierzu den KVen bei erstmaliger Einrichtung der Teilnehmer, regelmäßig monatlich zum 15. des Folgemonats und ansonsten unverzüglich bei Änderungen oder Erweiterungen des Teilnehmerkreises eine Auflistung der in den Netzkopplungsroutern eingerichteten Teilnehmer zur Verfügung.

Die Aufstellung hat pro KV zu erfolgen und ist ausschließlich an die betreffende KV zu melden und enthält die folgenden Informationen:

- Nachname und Vorname des Teilnehmers
- Gebiet der KV-Zugehörigkeit des Teilnehmers
- Lebenslange Arztnummer (LANR) des Teilnehmers, falls der Teilnehmer eine LANR besitzt
- Betriebsstättennummer (BSNR) des Teilnehmers, falls der Teilnehmer eine BSNR besitz
- zu nutzende Anwendungen oder Begründung für den Zugang zum *Sicheren Netz der KVen*

Da die KVen den Teilnehmerkreis bestimmen, sind diese auch in der Pflicht, den Teilnehmerkreis zu prüfen. Diese Prüfung sollte regelmäßig bei Änderung des Teilnehmerkreises durchgeführt werden, mindestens aber jährlich.

Das Datenformat zur Übermittlung der Statistiken ist in der Anhang A dieser Richtlinie verbindlich definiert.

10 Salvatorische Klausel

Sollten Teile oder einzelne Formulierungen dieser Richtlinie aus irgendeinem Grund ungültig sein, bleiben die übrigen Teile des Dokuments in ihrem Inhalt und ihrer Gültigkeit unberührt.

11 Glossar

Begriff	Erklärung
Anbieternetz	Zum Netz des Anbieters zählen alle notwendigen Dienste und Infrastrukturelemente, die zur Einrichtung, Aufrechterhaltung und Wartung der KV-SafeNet Anbindung zwischen Teilnehmer und KV notwendig sind.
Applikation	Services und Anwendungen im *Sicheren Netz der KVen*
Applikationsanbieter	Anbieter eines Dienstes
Betreiber der anzuschließenden Netzinfrastruktur	Institution, die die im Rahmen der Netzkopplung anzuschließende Netzinfrastruktur verantwortet.
Dienstenetz (DN)	Das Dienstenetz ist das Netz der Services und Anwendungen. Hier werden alle Anwendungsserver des *Sicheren Netzes der KVen* installiert und verfügbar gemacht. Die Organisation des Dienstenetzes liegt in der Verantwortung der Applikationsanbieter bzw. des Rechenzentrumsdienstleisters.
Einwahlknoten / Konzentrator	Der Einwahlknoten ist der Endpunkt des Anbieternetzes, der in der KV installiert ist und den Übergang vom Anbieternetz zum *Sicheren Netz der KVen* darstellt.
Firewall	Eine Firewall dient dazu, den Netzwerkzugriff zu beschränken, basierend auf Absender- oder Zieladresse und genutzten Diensten. Die Firewall überwacht den durch sie hindurch laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden, oder nicht. Auf diese Weise versucht die Firewall unerlaubte Netzwerkzugriffe zu unterbinden.
Firmware	Firmware bezeichnet Software, die in elektronische Geräte fest eingebettet und somit mit dem Gerät untrennbar verbunden ist. Eine Firmware benötigt u.U. in regelmäßigen Abständen ein Update.
Fremdprovider / VPN-Provider	Ein VPN-Provider stellt im Gegensatz zum ISDN, DSL oder UMTS Provider nicht die technischen Voraussetzungen bzgl. der Übertragungstechnik zur Verfügung, sondern nutzt eine bereits bestehende Internetverbindung.
KV-App	Siehe Applikation.
KV-Backbone	Der KV-Backbone ist ein geschütztes, logisch vom Internet getrenntes, vollvermaschtes VPN-Netzwerk auf Basis eines von der KBV definierten Konzeptes. Die Rechenzentren der Kassenärztlichen Vereinigungen (KVen) und der Kassenärztlichen Bundesvereinigung (KBV) sind über den KV-Backbone miteinander vernetzt. Die KBV ist der Betreiber des KV-Backbones.
KV-FlexNet	Anbindungsmöglichkeit eines Teilnehmers an das *Sichere Netz der KVen* mittels einer Software-VPN-Lösung. Der Anschluss erfolgt über die KV des Teilnehmers.
KV-SafeNet	Anbindungsmöglichkeit eines Teilnehmers an das *Sichere Netz der KVen* mittels einer Hardware-VPN-Lösung, dem KV-SafeNet-Router. Der Anschluss erfolgt über einen KV-SafeNet-Provider.
KV-SafeNet-Provider	Von der KBV nach der KV-SafeNet-Richtlinie zertifizierter Provider, der Teilnehmern einen Zugang über die Anschlussvariante „KV-SafeNet“ zum *Sicheren Netz der KVen* ermöglicht.

Begriff	Erklärung
KV-SafeNet-Router	Ein KV-SafeNet-Router ist ein nicht manipulierbarer Router. Dieser wird zwischen Internetanschluss und Praxisnetzwerk geschaltet. Dieser Router baut ein virtuelles privates Netzwerk (VPN) zu einem Einwahlknoten in der KV auf, welches die Verbindung vom normalen Internet abschottet und so einen abgesicherten Datenaustausch mit dem *Sicheren Netz der KVen* ermöglicht. Gleichzeitig blockiert der Router den Zugriff von außen auf das Praxis-Netzwerk und die dortigen Daten, da er den Zugriff aus dem Anbieternetz in das Teilnehmernetz verhindert. Die Verantwortung für den KV-SafeNet-Router trägt der KV-SafeNet-Provider.
Netzkopplungsprovider	Von der KBV nach der Richtlinie KV-SafeNet (Netzkopplung) zertifizierter Anbieter, der die Netzkopplung durchführt und damit Teilnehmern aus angeschlossenen Netzinfrastrukturen einen Zugang zum *Sicheren Netz der KVen* ermöglicht. Siehe auch KV-SafeNet-Provider.
Netzkopplungsrouter	Ein Netzkopplungsrouter dient dem Anschluss größerer Netzinfrastrukturen an das *Sichere Netz der KVen*. Er wird von einem Netzkopplungsprovider bereitgestellt. Ein Netzkopplungsrouter ist ein nicht manipulierbarer Router. Dieser Router baut ein virtuelles privates Netzwerk (VPN) zu einem Einwahlknoten in der KV auf, welches die Verbindung vom normalen Internet abschottet und so einen abgesicherten Datenaustausch mit den Rechenzentren der jeweiligen KV und der KBV ermöglicht. Teilnehmer aus der angeschlossenen Netzinfrastruktur müssen sich vor einem Zugriff auf *Das Sichere Netz der KVen* am Netzkopplungsrouter mit sicheren Verfahren authentifizieren. Die Zugriffe auf das *Sichere Netz der KVen* werden protokolliert. Die Verantwortung für den Netzkopplungsrouter trägt der Provider.
Servicenetz	Siehe Dienstenetz
Sicheres Netz der KVen	Das *Sichere Netz der KVen* ist eine von der KBV und den KVen bereitgestellte Infrastruktur, bestehend aus einem vollvermaschten VPN-Netzwerk (KV-Backbone), im Netzwerk befindlichen Diensten und Anwendungen (KV-Apps) und den definierten Anbindungsmöglichkeiten an das Netzwerk (KV-SafeNet und KV-FlexNet). Diese Infrastruktur trägt den Anforderungen an Datenschutz und Datensicherheit Rechnung und ist für die Übermittlung von Sozialdaten geeignet.
Teilnehmer	Ein Teilnehmer ist ein Vertragsarzt, -psychotherapeut oder ein anderes nach den Richtlinien der KBV zugelassenes Mitglied des *Sicheren Netzes der KVen*. Grundsätzlich bestimmen die KVen den Teilnehmerkreis.
Teilnehmernetz	Die untereinander lokal vernetzten Teilnehmercomputer bilden das Netzwerk des Teilnehmers. Hier können sich weitere vernetzte Endsysteme (z.B. Server, Drucker, Kartenleser) befinden.
Transfernetz (TFN)	Das Transfernetz dient der Weiterleitung der Datenpakete vom Teilnehmer zu den Applikationsservern und zurück. Es wird durch den KV-Backbone-Router realisiert. Die Organisation des Transfernetzes liegt in Verantwortung des KV-Backbone-Betreibers.
Tunnel / VPN-Tunnel	Für die Kommunikation des zugeordneten Netzes mit einem seiner VPN-Partner werden am VPN-Gateway die ursprünglichen Netzwerkpakete in ein VPN-Protokoll gepackt. Daher spricht man bei VPN vom Tunnel.
Zertifizierung	Prozess in dem explizit nachgewiesen wird, wie der Antragsteller die in der Richtlinie geregelten Anforderungen umsetzt. Wird dieses Verfahren erfolgreich abgeschlossen, erhält der Antragsteller eine Konformitätserklärung.
Zugangsnetz	Dazu gehören Netzelemente und Vermittlungsstellen, die Grundlagen der techn. Infrastruktur zwischen Anbieter- und Teilnehmeranschluss schaffen.

12 Referenzierte Dokumente

Referenz	Dokument
[KBV_SNK_RLEX_KV-SafeNet]	Richtlinie KV-SafeNet
[KBV_SNK_RLKV_KV-Apps]	Richtlinie KV-Apps
[KBV_SNK_KNEX_DNS]	Konzept DNS
[KBV_SNK_KNEX_Routing]	Konzept Routing
[KBV_SNK_KNEX_IP-Adressvergabe]	Konzept IP-Adressvergabe
[KBV_SNK_LFEX_Zert_KV-SafeNet]	Leitfaden Zertifizierung KV-SafeNet-Provider
[KBV_SNK_LFEX_Zert_Netzkopplung]	Leitfaden Zertifizierung Netzkopplungsprovider
[KBV_SNK_LFEX_Überprüfung_Provider]	Leitfaden Überprüfung Provider
[KBV_SNK_MBEX_Sicherheit_Arbeitsplätze]	Merkblatt Sicherheitsanforderungen an KV-SafeNet-Arbeitsplätze
[KBV_SNK_FOEX_Netzkopplung]	Formular Ergänzende Erklärung zur Zertifizierung zum Netzkopplungsprovider

A N H A N G

A Einheitliche Meldestruktur der Statistiken

Die folgenden Anschnitte beschreiben die von der Richtlinie KV-SafeNet abweichend zu liefernden Informationen.

A.1 Datendurchsatz

A.1.1 Dateinamenskonvention

<Dateiname> ::= 'datendurchsatz' . 'p' <ProviderID> . <Jahr> . <Monat>. 'csv'

Dateiname der Datendurchsatz-Meldung

<ProviderID> ::= 001 | 002 | 003 ... | 999

Eindeutige ID des KV-SafeNet-Providers; entspricht den letzten drei Stellen der Prüfnummer gemäß Zulassungsliste KV-SafeNet-Provider

<Jahr> ::= 2000...2099

Jahr der Meldung

<Monat> ::= 01 | 02 | 03 | ... | 10 | 11 | 12

Monat der Meldung

A.1.2 Datensatzbeschreibung

<Meldungen> ::= <Meldung> { 'CRLF' <Meldung> }

Datei mit einer Liste von Meldungs-Einträgen

<Meldung> ::= <ProviderID> ; <BetreiberID>; <IP-Adresse> ; <Datendurchsatz>

Auflistung des Datendurchsatzes pro Netzkopplungsrouter

<ProviderID> ::= 001 | 002 | 003 ... | 999

Eindeutige ID des KV-SafeNet-Providers; entspricht den letzten drei Stellen der Prüfnummer gemäß Zulassungsliste[7] KV-SafeNet-Provider

<BetreiberID> ::= <text>

Freitext für die Bezeichnung des Betreibers der anzuschließenden Netzinfrastruktur.

<IP-Adresse> ::= 188 . (144 | 145) . (0...254) . (0...254)

[7] http://daris.kbv.de/daris/link.asp?ID=1003760655

Öffentliche SafeNet-IP-Adresse des Anschlusses

<Datendurchsatz> ::= <zahl>

Datendurchsatz des betreffenden Netzkopplungsrouters in MByte

A.2 Teilnehmerstatistiken für die KBV

A.2.1 Dateinamenskonvention

<Dateiname> ::= 'teilnehmernuebersicht' . 'p' <ProviderID> . <Jahr> . <Monat> .<tag>. 'csv'

Dateiname der monatlichen Teilnehmerstatistik für die KBV

<ProviderID> ::= 001 | 002 | 003 ... | 999

Eindeutige ID des KV-SafeNet-Providers; entspricht den letzten drei Stellen der Prüfnummer gemäß Zulassungsliste KV-SafeNet-Provider (vgl. http://daris.kbv.de/daris/link.asp?ID=1003760655)

<Jahr> ::= 2000...2099

Jahr der Meldung

<Monat> ::= 01 | 02 | 03 | ... | 10 | 11 | 12

Monat der Meldung

<Tag> ::= 01 | 02 | 03 | ... | 29 | 30 | 31

Tag der Meldung

Beispiel:
monatsstatistik.p18.2011.07.01.csv → PROVIDER ABC an KBV vom 1. Juli 2011

A.2.2 Datensatzbeschreibung

<Meldungen> ::= <Meldung> { 'CRLF' <Meldung> }

Datei mit einer Liste von Meldungs-Einträgen

<Meldung> ::= <ProviderID> ; <BetreiberID>; <TypNetzkopplungsRouter><AnzahlTeilnehmer>

Auflistung der Meldungsparameter

<ProviderID> ::= 001 | 002 | 003 ... | 999

Eindeutige ID des KV-SafeNet-Providers; entspricht den letzten drei Stellen der Prüfnummer gemäß Zulassungsliste[8] KV-SafeNet-Provider.

<BetreiberID> ::= <text>

Freitext für die Bezeichnung des Betreibers der anzuschließenden Netzinfrastruktur.

[8] http://daris.kbv.de/daris/link.asp?ID=1003760655

<TypNetzkopplungsRouter> ::= <text>

Freitext für die Bezeichnung des Netzkopplungsrouters

<AnzahlTeilnehmer> ::= <numerischerWert>

Numerischer Wert: Anzahl der Teilnehmer, die über einen Netzkopplungsanschluss aus der Netzinfrastruktur des Betreibers an das *Sichere Netz der KVen* angeschlossen

A.3 Teilnehmerübersichten

A.3.1 Dateinamenskonvention

<Dateiname> ::= 'teilnehmeruebersicht' . 'p' <ProviderID> . 'kv' <KVID> . <Jahr> . <Monat> .<tag>. 'csv'

Dateiname der Teilnehmerübersicht.

<ProviderID> ::= 001 | 002 | 003 ... | 999

Eindeutige ID des KV-SafeNet-Providers; entspricht den letzten drei Stellen der Prüfnummer gemäß Zulassungsliste KV-SafeNet-Provider (vgl. http://daris.kbv.de/daris/link.asp?ID=1003760655)

<KVID> ::= 01 | 02 | 03 | ... | 99

KV-Nummer der KV[9], die den Teilnehmer anerkannt hat bzw. anerkennen soll

<Jahr> ::= 2000...2099

Jahr der Meldung

<Monat> ::= 01 | 02 | 03 | ... | 10 | 11 | 12

Monat der Meldung

<Tag> ::= 01 | 02 | 03 | ... | 29 | 30 | 31

Tag der Meldung

Beispiel:
teilnehmeruebersicht.p18.kv02.2011.07.01.csv → PROVIDER ABC an KV XYZ vom 1. Juli 2011

A.3.2 Datensatzbeschreibung

<Meldungen> ::= <Meldung> { 'CRLF' <Meldung> }

Datei mit einer Liste von Meldungs-Einträgen

<Meldung> ::= <ProviderID> ; <Version> ; <KVID> ; <BetreiberID>; <Name>; <Vorname>; <BSNr> ; <LANr> ; <IP-Adresse> ; <Beginn> ; [<Ende>]

[9] http://www.kbv.de/keytabs/ita/schluesseltabellen.asp?page=S_KBV_KV_V1.05.htm

Auflistung der Meldungsparameter je Teilnehmer

<ProviderID> ::= 001 | 002 | 003 ... | 999

Eindeutige ID des KV-SafeNet-Providers; entspricht den letzten drei Stellen der Prüfnummer gemäß Zulassungsliste[10] KV-SafeNet-Provider.

<Version> ::= 1.0 | ...

Version der Richtlinie KV-SafeNet (Netzkopplung), zu der der Vertrag geschlossen wurde / gilt

<KVID> ::= 01 | 02 | 03 | ... | 99

KV-Nummer der KV[11], die den Teilnehmer anerkannt hat bzw. anerkennen soll.

<BetreiberID> ::= <text>

Freitext für die Bezeichnung des Betreibers der anzuschließenden Netzinfrastruktur.

<Name> ::= <text>

Freitext für den Namen des Teilnehmers

<Vorname> ::= <text>

Freitext für den Vornamen des Teilnehmers

<BSNr> ::= 010000000...999999999 | „“

Neunstellige Betriebsstättennummer der Praxis / Einrichtung, falls verfügbar

<LANr> ::= 010000000...999999999 | „“

Neunstellige „Lebenslange Arztnummer“ des Teilnehmers, falls verfügbar

<IP-Adresse> ::= 188 . (144 | 145) . (0...254) . (0...254)

Öffentliche SafeNet-IP-Adresse des Anschlusses

<Beginn> ::= (1...31) . (1...12) . (2000...2099)

Datum des Vertragsbeginns (Tag.Monat.Jahr)

<Ende> ::= (1...31) . (1...12) . (2000...2099)

Beispielinhalt teilnehmeruebersicht.p001.kv02.2011.07.01.csv (Provider an KVHH vom 1. Juli ´11)

18; 1.0; 02; Krankenhaus1; Mueller; Frank; 021234564; 111222333; 188.144.179.132; 24.02.2009;22.04.2011

[10] http://daris.kbv.de/daris/link.asp?ID=1003760655
[11] http://www.kbv.de/keytabs/ita/schluesseltabellen.asp?page=S_KBV_KV_V1.05.htm

18;1.0;02;Krankenhaus1;Schmidt; Anita; 024445555; 081547110; 188.144.179.144; 04.12.2007; 31.03.2009